UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

United States of America,	)	**CASE NO. 1:16 CR 236**
	)	
Plaintiff,	)	**JUDGE PATRICIA A. GAUGHAN**
	)	
Vs.	)	
	)	
Adam Libbey-Tipton,	)	**Memorandum of Opinion and Order**
	)	
Defendant.	)	

INTRODUCTION

This matter is before the Court upon defendant's Motion to Suppress Evidence (Doc. 14). For the reasons that follow, the motion is DENIED.

FACTS

Defendant is charged with two counts of possession of child pornography.

On or about February 20, 2015, the government obtained an order from the Eastern District of Virginia allowing it to seize control of the operation of "Website A." Website A contains various sections and forums related to child pornography. Website A requires users to install publically available computer software before accessing the site. The software prevents

someone attempting to monitor the internet connection from learning the user's physical location by routing communications through other locations. In this way, law enforcement cannot ascertain through public lookups the location of the users of Website A.

Pursuant to the Virginia warrant, the government was authorized to deploy a Network Investigative Technique ("NIT"). Each time a user logged onto Website A with a username and password, the FBI deployed the NIT which sent signals to the user's computer. Those communications were designed to cause the user's computer to deliver information to the government that identified the actual location of the user. The information included, among other things, the user's actual IP address.

On or about March 3, 2015, and based on the information received by the FBI pursuant to the Virginia warrant (sometimes "NIT warrant"), the government identified an individual with a user name "Revenger." According to the government, Revenger accessed a number of posts on Website A containing child pornography. As a result of the NIT, the government learned the IP address used by Revenger. Using publicly available websites, government agents discovered that AT&T Uverse operates the IP address used by Revenger. After issuing an administrative subpoena to AT&T Uverse, the government learned the physical address associated with the IP address. It appears that the account is in the name of "Stacey Irace," and the preferred email address associated with the account is "AdamL_T@yahoo.com." The government determined through various records that defendant resides at the location associated with the IP address (the "Premises"). The government also learned that defendant is a registered sex offender.

In the connection with the NIT warrant, the government obtained authorization to delay providing notification of the targets of the NIT search for a period of "30 days after any

individual accessing [Website A] has been identified to a sufficient degree as to provide notice..." According to defendant, the court did not extend the 30-day delayed notification provisions. On July 31, 2015, the government obtained a search warrant in this District to search the Premises. On August 7, 2015, the FBI executed that search warrant. Defendant claims that the government never informed him that they previously searched his computer as a result of the NIT warrant.

On July 27, 2016, defendant was indicted for possession of child pornography. Defendant moves to suppress evidence obtained as a result of the NIT warrant and all other evidence obtained as "fruit of the poisonous tree." The government opposes the motion.

ANALYSIS

Rule 41(b)

Defendant argues that the NIT warrant violates Rule 41(b) of the Federal Rules of Criminal Procedure. That rules provides:

Venue for a Warrant Application. At the request of a federal law enforcement officer or an attorney for the government:

> (1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
>
> (3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
>
> > (A) a United States territory, possession, or commonwealth;
> >
> > (B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
> >
> > (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

According to defendant, the NIT warrant was not properly issued under subsection (b)(1) or any of the other aforementioned subsections. As such, defendant argues that the violation of Rule 41 requires suppression. In response, the government argues that the NIT warrant complied with Rule 41. In the alternative, the government argues that even if the Magistrate Judge lacked authority to issue the warrant it does not rise to a constitutional violation. Regardless, suppression would not be warranted under the good-faith exception.

Upon review, the Court finds that the NIT warrant was not properly issued pursuant to Rule 41. The government relies primarily on subsection 41(b)(4) in support of its position that the Magistrate Judge had jurisdiction to issue the warrant. That rule allows a Magistrate Judge to issue a warrant to "install within the district a tracking device." The device may be used to "track the movement of a person or property located within the district, outside the district, or both."

As an initial matter, this issue has come before a number of district courts addressing this

very warrant. Some courts have held that subsection (b)(4) does not apply because the "tracking device" was not "installed" in Virginia. For example, in *United States v. Michaud*, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016), the court determined that the Magistrate Judge lacked jurisdiction:

> If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [defendant's] computer, applying the tracking device exception again fails, because [defendant] was never physically located within the Eastern District of Virginia.

See also, United States v. Ammons, –F.Supp.3d– , 2016 WL 4926438 (W.D. Ky. Sept. 14, 2016)("Even assuming the NIT qualifies as a 'tracking device,' the installation occurred not within the Eastern District of Virginia, but in the Western District of Kentucky where [defendant's] computer was located.").

Other courts have determined that regardless of where the installation occurred, the NIT is not a "tracking device" making reliance on Rule 41(b)(4) improper:

> Again, I am not persuaded by the government's argument. While it is tempting to view the NIT as a tracking device, the reality of the technology at issue here is that the NIT did not 'track the movement of...property' as Rule 41(b)(4) contemplates. The government did not obtain [defendant's] IP address by tracking the data as it moved through various relay nodes back to [defendant's] computer. Rather, the government, through the NIT, searched [defendant's] computer and seized his IP address along with various other pieces of information. As such, Rule 41(b)(4) is inapplicable.

United States v. Workman, 2016 WL 5791209 (D. Colo. Sept. 6, 2016). *See also, United States v. Adams*, 2016 WL 4212079 (M.D.Fla. Aug. 10, 2016)("the NIT does not track; it searches"); *United States v. Levin*, –F.Supp.3d–, 2016 WL 2596010 (D. Mass. May 5, 2016)(court not convinced that NIT may properly be considered "tracking device" regardless of where installation occurred).

On the other hand, some courts have concluded that the NIT constitutes a tracking device that the government installed in Virginia and, as such, the Magistrate Judge properly issued the warrant pursuant to Rule 41(b)(4). By and large, those cases hold that users located outside of Virginia entered the state by accessing Website A. When a user downloaded child pornography, the government placed a "tracking device" in the form of computer code on that child pornography. The child pornography, along with the attached tracking device, then traveled to Ohio. Once in Ohio, the computer code entered the user's computer and returned information disclosing the user's location. As such, the NIT acted as a typical tracking device. For example, in *United States v. Darby*, –F.Supp.3d–, 2016 WL 3189703 (E.D. Va. June 3, 2016), the court held as follows:

> Users of [Website A] digitally touched down in the Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location.

Similarly, in *United States v. Jean*, the court thoroughly analyzed whether subsection (b)(4) applies. The court indicated that pursuant to Rule 41(a)(2), a "tracking device" is an "electronic or mechanical device which permits the tracking of the movement of a person or object." Subsection (b)(4) allows for the tracking of "property," which includes "information." The court noted that, although "device" is not defined, it is commonly understood to mean a "tool or technique" used to do a task. As such, the court determined:

> First, the NIT is an 'electronic device' within the meaning of 18 U.S.C. § 3117(b), because it is an investigative tool consisting of computer code transmitted electronically over the internet. Second, the purpose of the NIT was to track the movement of 'property'–which in this case consisted of intangible 'information,' something expressly contemplated by the definition in Rule 41(a)(2)(A).
>
> The court further had no difficulty determining that the "tracking device" was installed in

Virginia:

> It is undisputed that the NIT authorized by the warrant was executed by the FBI from its computer located within Virginia. It is also undisputed that but for [defendant] electronically traveling in search of child pornography to the watering hole in Virginia, the NIT could not have been deployed. Thus, on the facts of this case, the only reasonable interpretation of where the information-tracking NIT was 'installed' for purposes of Rule 41(b)(4), is the Eastern District of Virginia, where the tracking device–in this case a string of computer code– was caused to be executed and deployed.

See also, United States v. Matish, –F.Supp.3d–, 2016 WL 3545776 (E.D. Va. June 23, 2016)(when user's computer "left" Virginia, the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target's location); *United States v. Laurita*, 2016 WL 4179365 (D. Neb. Aug. 5, 2016)("the NIT enabled the government to determine the website user's locations by installing a tracking device on each user's computer when that computer in essence traveled into the district").

Although the Court finds it to be a close call, the Court agrees with the line of cases holding that the NIT warrant was not properly issued under Rule 41(b)(4). Assuming *arguendo* that the government installed the NIT in Virginia by "attaching" computer code to the pornographic image, the Court is not convinced that the computer code constitutes a "tracking device." Although the court agrees with *Jean* that in some instances "techniques" can constitute "devices," the nature of the NIT cautions against such a finding in this case. The computer code deployed by the government entered a user's computer and overrode software on the device that disabled location features. It also "took over" the computer in the sense that it "instructed the computer to deliver...data...includ[ing] the computer's actual IP address, and the date and time that the NIT determined what the IP address was; a unique identifier generated by the NIT, the type of operating system run on the computer, information about whether the NIT had already

been delivered to the computer, the computer's host name, the computer's active operating system username, and the computer's MAC address." The Court is doubtful that this "technique" constitutes a "tracking device" as contemplated by Rule 41(b)(4). The Court's determination is bolstered by the fact that the Supreme Court recently approved an amendment to Rule 41(b) in order to address this precise situation. Rather than augment subsection (b)(4) to clarify that NIT-type technology constitutes a "tracking device," the proposed rule contains an entirely new subsection directed specifically at warrants to "use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if...the district where the media or information is located has been concealed through technological means." Proposed Rule 41(b)(6)(a). In all, the Court cannot say that the Magistrate Judge had authority to issue the NIT warrant based on Rule 41(b)(4).

The Court also rejects the government's argument that either subsection 41(b)(1) or 41(b)(2) is satisfied here. Subsection (b)(2) confers upon a Magistrate Judge the "authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Here, the government claims that the NIT constitutes "property" located in the Eastern District of Virginia. The Court disagrees. The government's argument makes little sense when read in conjunction with the statute. Subsection (b)(2) is directed at situations in which the property is located in the district at the time the warrant is issued, but might move to outside the district before the warrant is executed. The NIT itself, *i.e.*, the computer code, is not the *object* of the warrant. Rather, the object of the warrant is the identifying information sent from a user's computer as a result of the deployment of the

computer code through the NIT. Surely the government is not concerned that the NIT itself might "move outside the district" *before* the warrant is issued. Accordingly, this provision is not applicable.

Subsection (b)(1) affords a Magistrate Judge the authority to "issue a warrant to search for and seize a person or property located within the district." The Court finds that this subsection is inapplicable as well. It is undisputed –and in fact problematic for government agents–that the information it seeks is *not* located in the Eastern District of Virginia. The government is understandably frustrated by users' successful attempts to obfuscate their identities for criminal purposes. The entire purpose of the warrant is to solve this problem. The government seized control of Website A and operated it out of the Eastern District of Virginia, but remained unable to discern the users' identities. Because the NIT warrant was not directed at obtaining information located within the district, the Magistrate Judge was without jurisdiction to issue the warrant pursuant to subsection (b)(1).

The government argues that any violation of Rule 41(b) is technical in nature and does not rise to the level of a constitutional violation. In the alternative, the government claims that suppression is not warranted in any event. Upon review, the Court finds that assuming *arguendo* the failure to comply with Rule 41 results in a constitutional violation, suppression is not warranted. In *United States v. Masters*, 614 F.3d 236 (6th Cir. 2010), the Sixth Circuit addressed a warrant issued by a state court judge. There, a sheriff's investigator obtained a warrant to search a residence thought to be located in Franklin County, Tennessee. The judge who signed the warrant had authority to issue warrants only in that county. Later, it was learned that the residence is actually located in Coffee County, not Franklin County. The Sixth Circuit held that,

pursuant to Tenn. R. Crim. Pro. 41(a), the judge that signed the warrant lacked the authority to issue the warrant to search defendant's Coffee County residence. Because the judge lacked authority to issue the warrant in the first place, the search violated defendant's Fourth Amendment rights.

The court went on to address whether the good faith exception enunciated in *United States v. Leon*, 468 U.S. 897 (1984), could be applied to instances in which void warrants are issued. The court discussed its prior decision in *United States v. Scott*, 260 F.3d 512, 515 (2001):

> In *Scott*, this Court specifically found that when a warrant is signed by someone who lacks legal authority necessary to issue warrants, the warrant is void *ab initio*. The Court specifically rejected the applicability of *Leon* in that case because *Leon* itself left untouched the probable-cause standard and the various requirements of a valid warrant. At the core of these various requirements is that the warrant be issued by a neutral and detached judicial officer.

Masters, 614 F.3d at 241

The court, however, went on to expressly "clarify or modify" *Scott*:

> The holding of...recent Supreme Court cases does not directly overrule our previous decision in *Scott*. Nonetheless, we believe that the Supreme Court's evolving suppression rulings in Fourth Amendment cases require clarification or modification of our precedent in *Scott*.
>
> The Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, 'the benefits of deterrence must outweigh the costs.' In following the Supreme Court's approach with respect to the instant case, the costs of excluding the evidence would appear to outweigh any deterrent effect. This is so, in no small measure, because the *Herring* Court's emphasis seems weighed more toward preserving evidence for use in obtaining convictions, even if illegally seized, than toward excluding evidence in order to deter police misconduct unless the officers engage in 'deliberate, reckless, or grossly negligent conduct.'

Id. at 243 (citations omitted).

Here, the Court finds that suppression is not warranted because the costs of excluding the evidence strongly outweigh any deterrent effect on law enforcement.[1] Here, defendant in essence asks that all evidence against him be excluded. If the government's case is proven, however, defendant engaged in the downloading of child pornography on a number of occasions and took measures specifically designed to avoid detection. It is obvious that the cost of excluding the evidence is substantial. On the other hand, the Court finds a negligible, if any, deterrent effect on the conduct of law enforcement. Defendant does not argue that the warrant lacks probable cause or that any agent misstated facts or law in order to obtain the warrant. Although in passing, defendant claims that the government somehow attempted to cover up the fact that the users' computers are the actual "places to be searched," and, instead, attempted to claim that the place to be searched is Virginia. The Court disagrees. Having closely reviewed the warrant, affidavit in support, and the accompanying exhibits, the Court finds that the government disclosed the nature of the NIT, how the technology works, and the fact that the "activating computers" on which the NIT will be deployed are those of "any user or administrator who logs into [Website A]." Defendant fails to point to anything in the warrant that is untrue or misleading or suggest that any agent encouraged or invited the Magistrate Judge to misapprehend her jurisdiction.

Defendant also claims that the "officers acted in intentional and deliberate disregard of

---

[1] Both parties rely on Ninth Circuit law analyzing whether Rule 41 violations warrant suppression. Neither party cites to *Masters*, which is a Sixth Circuit decision analyzing whether suppression is warranted when a judge issues a warrant without jurisdiction to do so. The Court will apply the test enunciated in *Masters* in analyzing whether suppression is warranted.

Rule 41." According to defendant, Rule 41 plainly does not allow dragnet searches spanning the entire country. Again, the Court disagrees. As aptly noted in *Ammons, supra*, "[t]he FBI agents can hardly be faulted for failing to understand the intricacies of the jurisdiction of federal magistrates. After all, there is disagreement among reasonable jurists on that very question." *Ammons*, 2016 WL 4926438 at * 9 (citations and quotations omitted). Moreover, the exclusionary rule is designed "to curb police rather than judicial misconduct." *Master*, 614 F.3d at 242. Here, the Court finds that suppression is unwarranted. To do so would cause the exclusion of reliable evidence bearing on guilt or innocence in exchange for little or no deterrent effect. Given the complete lack of police misconduct in securing the warrant, the Court finds that suppression is not warranted because the "good faith" exception to the exclusionary rule applies. *See also, United States v. Werdene*, 2016 WL 3002376 (E.D. Pa. May 18, 2016)(suppression not warranted); *United States v. Darby*, 2016 WL 3189703 (E.D. Va. June 3, 2016)(same); *United States v. Michaud*, 2016 WL 337263 (same); *United States v. Jean*, 2016 WL 4771096 (warrant did not violate Rule 41(b), but even if it did, suppression not warrant); *United States v. Matish*, 2016 WL 3545776 (E.D Va. June 23, 2016)(government not required to obtain warrant to deploy NIT, but suppression not warranted in any event under good faith exception).

Defendant also argues that the government violated Rule 41's notice requirements by failing to provide a copy of the warrant to defendant. The government does not respond to this argument. In this case, the Virginia court authorized a 30-day delayed notice period due to the ongoing nature of the investigation. According to defendant, the government did not provide a copy of the warrant until more than one year after the search occurred. Defendant argues that

this failure "further demonstrates the government's deliberate disregard of Rule 41." According to defendant, suppression is required. Upon review, the Court disagrees. Defendant wholly fails to argue as to why the failure to provide timely notice rises to the level of a constitutional violation. Nor does defendant claim that the late notice somehow rendered the search unreasonable. Defendant points to no prejudice he suffered as a result of any violation of Rule 41's notice requirements. And, although defendant claims that the violation was "intentional," the Court finds that any deterrent effect would be outweighed by the societal costs in excluding the evidence. For these reasons, defendant's late notice argument is rejected.

Because the Court finds that suppression is not required even accepting defendant's version of the facts, an evidentiary hearing is not warranted.

CONCLUSION

For the foregoing reasons, defendant's Motion to Suppress Evidence (Doc. 14) is DENIED.

IT IS SO ORDERED.

/s/ Patricia A. Gaughan
PATRICIA A. GAUGHAN
United States District Judge

Dated: 10/19/16